(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년09월13일
(11) 등록번호 10-2301742
(24) 등록일자 2021년09월07일

(51) 국제특허분류(Int. Cl.)
G07C 9/00 (2020.01) *G07C 9/20* (2020.01)
(52) CPC특허분류
G07C 9/00309 (2013.01)
G07C 9/00563 (2013.01)
(21) 출원번호 10-2021-0025378
(22) 출원일자 2021년02월25일
심사청구일자 2021년02월25일
(56) 선행기술조사문헌
KR1020170073109 A*
KR102124838 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
(주)케이스마텍
서울특별시 금천구 가산디지털1로 168, 에이동 1207호 (가산동, 우림라이온스밸리)
(72) 발명자
고인옥
경기도 김포시 풍무로68번길 41 한화유로메트로아파트, 209동 1303호(풍무동, 한화유로메트로)
김성원
경기도 부천시 조마루로 84 하얀마을현대아이파크 2607-1401
(뒷면에 계속)
(74) 대리인
김봉조

전체 청구항 수 : 총 8 항 심사관 : 류시웅

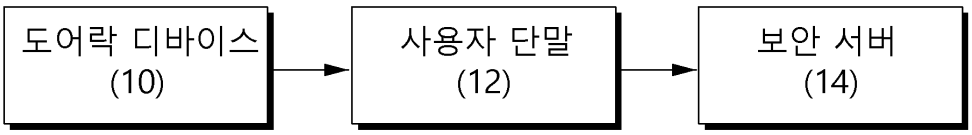
(54) 발명의 명칭 **키패드 없는 스마트 도어락 키 등록 및 사용방법과 그 출입관리 시스템**

(57) 요 약

키패드 없는 스마트 도어락 키 등록 및 사용방법과 그 출입관리 시스템이 개시된다. 일 실시 예에 따른 키패드 없는 스마트 도어락 키 등록 및 사용방법과 그 출입관리 시스템은, 도어락 앱이 설치된 사용자 단말을 이용하여 NFC 방식, 근거리 무선통신(UWB/BLE) 및 지문인식 방식을 통해 별도의 키 패드 없이도 사용자 단말을 가지고 도어락 디바이스를 잠금 해제한다.

대 표 도 - 도1

1



(52) CPC특허분류
G07C 9/00571 (2013.01)
G07C 9/20 (2020.01)
G07C 2009/00412 (2013.01)
G07C 2209/08 (2013.01)
G07C 2209/64 (2013.01)
(72) 발명자
황재형
경기도 성남시 분당구 동판교로 275 봇들마을1단지 신미주아파트 115동 704호
안재성
인천광역시 부평구 부흥북로 48 아미파크뷰
이동준
서울특별시 노원구 공릉로34길 62 태강아파트 1003동 706호

명 세 서

청구범위

청구항 1

사용자 단말이 도어락 앱을 실행하는 단계;

사용자 단말이 사용자 조작에 의해 도어락 키 등록을 위한 사용자 인증정보를 입력 받는 단계;

사용자 단말이 사용자 인증정보를 암호화하고 암호화된 사용자 인증정보를 보안 서버에 전송하는 단계;

보안 서버가 사용자 인증정보를 검증하고 검증이 이루어지면 도어락 키를 생성하여 사용자 단말의 보안영역에 주입하는 단계; 및

사용자 단말 및 도어락 디바이스 간의 근거리 무선통신을 통해 도어락 디바이스에 도어락 키를 저장하는 단계; 를 포함하고,

사용자 단말은 일반영역 및 보안영역을 포함하고,

상기 암호화된 사용자 인증정보를 보안 서버에 전송하는 단계는

일반영역이 보안영역에 S/N 암호화 및 키 생성을 요청하는 단계;

보안영역에서 앱 공개키 및 앱 개인키를 포함하는 앱 키 쌍을 생성하고 서버 공개키로 앱 공개키 및 도어락 S/N를 암호화하는 단계;

보안영역이 암호화된 앱 공개키 및 도어락 S/N를 일반영역에 전달하는 단계; 및

일반영역이 전달받은 암호화된 앱 공개키 및 도어락 S/N를 보안 서버에 전달하는 단계;

를 포함하는 것을 특징으로 하는 도어락 키 등록방법.

청구항 2

제 1 항에 있어서, 상기 사용자 인증정보를 입력 받는 단계는

사용자가 사용자 단말을 이용하여 도어락 디바이스에 포함된 QR 코드를 촬영하거나 도어락 디바이스에 기입된 도어락 S/N을 직접 입력하는 방식을 통해 사용자 인증정보를 입력 받는 것을 특징으로 하는 도어락 키 등록방법.

청구항 3

삭제

청구항 4

제 1 항에 있어서,

보안 서버는 제어부; 하드웨어 보안 모듈(Hardware Security Module: HSM, 이하 'HSM'이라 칭함); 및 DB; 를 포함하고,

상기 사용자 단말의 보안영역에 주입하는 단계는

제어부가 사용자 단말로부터 수신된 앱 공개키 및 도어락 S/N의 복호화를 HSM에 요청하는 단계;

HSM이 서버 개인키로 앱 공개키 및 도어락 S/N을 복호화 하여 앱 공개키 및 도어락 S/N을 확인하고 확인된 앱 공개키 및 도어락 S/N을 제어부에 전달하는 단계;

제어부가 DB에서 도어락 S/N 및 도어락 공개키를 확인하고, 도어락 S/N이 존재하면 HSM에 도어락 키 생성을 요청하는 단계;

HSM이 요청에 따라 도어락 키를 생성하고, 생성된 도어락 키를 도어락 공개키로 암호화하며, 생성된 도어락 키

및 도어락 공개키를 앱 공개키로 암호화하는 단계;

HSM이 암호화된 도어락 키 및 도어락 공개키를 제어부에 전달하는 단계; 및

제어부가 암호화된 도어락 키 및 도어락 공개키를 사용자 단말에 주입하는 단계;

를 포함하는 것을 특징으로 하는 도어락 키 등록방법.

청구항 5

도어락 디바이스가 활성화 모드에 진입하면 미리 설정된 시간 동안 미리 설정된 시간간격으로 근거리 무선통신 스캐닝 및 NFC 폴링을 수행하는 단계;

도어락 디바이스가 도어락 앱을 통한 사용자 단말의 접근을 감지하는 단계;

사용자 단말 및 도어락 디바이스 간에 NFC 태깅 또는 근거리 무선통신 페어링 되는 단계; 및

인증 데이터 생성 및 검증을 통해 도어락 디바이스가 잠금 해제되는 단계;

를 포함하고,

상기 도어락 디바이스가 잠금 해제되는 단계는

도어락 디바이스가 사용자 단말에 랜덤 값 생성 및 인증을 요청하는 단계;

사용자 단말이 랜덤 값을 생성하고 랜덤 값 및 도어락 키로 서명 값을 생성하고, 인증 데이터를 생성하는 단계;

사용자 단말이 인증 데이터를 도어락 디바이스에 전달하는 단계; 및

도어락 디바이스가 수신된 인증 데이터를 도어락 개인키로 복호화 하고, 랜덤 값을 검증하며, 도어락 키를 검증하고 권한을 확인한 후, 검증을 모두 성공하면 인증이 완료되고 도어락 디바이스의 잠금을 해제하는 단계;

를 포함하는 것을 특징으로 하는 도어락 키 사용방법.

청구항 6

삭제

청구항 7

제 5 항에 있어서, 인증 데이터를 생성하는 단계는

랜덤 값, 도어락 키 및 서명 값을 도어락 공개키로 암호화하여 인증 데이터를 생성하는 것을 특징으로 하는 도어락 키 사용방법.

청구항 8

제 5 항에 있어서, 도어락 키 사용방법은

사용자 단말이 공유자 단말과 도어락 키를 영구, 기간설정 및 1회용으로 구분하여 공유하는 단계; 및

사용자 단말이 공유자 단말로부터 공유한 키를 회수하는 단계;

중 적어도 하나를 더 포함하는 것을 특징으로 하는 도어락 키 사용방법.

청구항 9

도어락 키에 의해 잠금 해제되는 도어락 디바이스;

도어락 앱을 실행하고 도어락 키를 사용하여 NFC 태깅, 근거리 무선통신 및 지문인식 중 적어도 하나를 통해 도어락 디바이스를 잠금 해제하며, 일반영역과는 분리된 보안영역에 도어락 키를 저장하는 사용자 단말; 및

사용자 단말을 등록하고 등록된 사용자 단말 내부에 보안영역을 활성화하며 사용자 단말의 요청에 따라 도어락 키를 생성한 후 생성된 도어락 키를 사용자 단말의 활성화된 보안영역에 주입하는 보안 서버;를 포함하고,

도어락 디바이스는 도어락 디바이스 내 보안 모듈에서 도어락 개인키 및 도어락 공개키를 포함하는 도어락 키 쌍을 생성하고, 도어락 개인키는 보안 모듈 내에 보관하며, 도어락 공개키와 도어락 S/N 쌍을 보안 서버에 전송

하고,

보안 서버는 HSM에서 서버 개인키 및 서버 공개키를 포함하는 서버 키 쌍을 생성하고, 서버 개인키는 HSM 내에 보관하며, 서버 공개키를 도어락 디바이스에 주입하는 것을 특징으로 하는 출입관리 시스템.

청구항 10

제 9 항에 있어서, 도어락 디바이스는

QR 코드 및 S/N 중 적어도 하나를 포함하는 사용자 인증정보가 기입되고, 근거리 무선통신 등록 버튼 및 지문 등록 버튼을 구비하며,

사용자 단말의 도어락 앱과의 NFC 태깅을 통해 도어락 디바이스를 잠금 해제하는 NFC 리더기;

사용자 단말의 도어락 앱과의 근거리 무선통신을 통해 도어락 디바이스를 잠금 해제하는 근거리 무선통신 모듈; 및

사용자의 지문인식에 의해 도어락 디바이스를 잠금 해제하는 지문인식 센서;

를 포함하는 것을 특징으로 하는 출입관리 시스템.

청구항 11

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 키패드 없는 스마트 도어락 키를 이용한 출입관리 기술에 관한 것으로서, 더욱 상세하게는 하드웨어 기반의 보안환경과 소프트웨어 기반의 보안환경을 지원하는 사용자 단말을 사용하여 카드 키를 소지하지 않더라도 건물출입시 게이트 출입을 가능하게 할 수 있을 뿐만 아니라 사용자 편의를 향상시킬 수 있는 기술에 관한 것이다.

배 경 기 술

[0003] 최근 들어 무선통신기술이 급격히 발전하면서 NFC(Near field communication)와 같은 근거리 무선통신 기술을 이용하는 잠금 해제용 NFC 무선 카드 키 기술이 다양한 분야에서 각광을 받고 있다.

[0004] 종래기술에 따른 NFC 방식의 무선 카드 키 기술은 출입 게이트의 문을 잠금 해제하기 위해서 NFC 방식의 카드 키를 반드시 소지해야 하며 카드 키를 가지고 있으면 누구나 해당 도어의 문을 열 수 있다.

[0005] 이와 같이 NFC 방식의 카드 키를 구비하여 출입 게이트를 잠금 해제하는 방식은 무선 카드 키를 소지한 자에게 모든 접근권한이 주어질 수 있기 때문에 카드 키를 분실하는 경우 사용자의 관리를 벗어나는 문제점이 있으며, 출입용 카드를 반드시 소지해야 하는 문제점이 있었다.

[0006] 한편, 최근 들어 정보통신 기술이 발전하면서 스마트폰과 같은 사용자 단말기에 설치되는 어플리케이션을 이용하여 무선으로 잠금 해제 대상을 제어하기 위한 노력이 시도되고 있다.

[0007] 그러나, 이와 같이 스마트폰과 같은 사용자 단말을 사용하는 경우에는 어플리케이션 설치에 따른 도어락 키 등록과정에서 보안을 안정적으로 확보하기 어려운 문제점이 있었다.

[0008] 뿐만 아니라, 사용자 단말에서 지원하는 보안환경이 다를 경우에 사용자 단말기의 특정 기종에 대해서는 적용하기가 어려운 문제점이 있었다.

[0009] 따라서, 사용자 단말을 이용해 카드 키가 없더라도 게이트 출입을 위한 도어락 키를 발급받을 수 있게 함으로써 사용자 편의성을 향상시킬 수 있으면서도 기종에 관계없이 보안성을 높일 수 있는 현실적이고도 적용이 가능한 출입관리 시스템에 관한 기술이 절실히 필요한 실정이다.

선행기술문헌

특허문헌

[0011] (특허문헌 0001) 대한민국공개특허공보 10-2013-0115557호 (공개일. 2013년10월22일)

발명의 내용

해결하려는 과제

[0012] 일 실시 예에 따라, 하드웨어 기반의 보안환경과 소프트웨어 기반의 보안환경을 지원하는 스마트폰을 사용하여 카드 키를 소지하지 않더라도 건물출입시 게이트 출입을 가능하게 할 수 있을 뿐만 아니라 사용자 편의를 향상시킬 수 있는 도어락 키 등록 및 사용방법과 그 출입관리 시스템을 제안한다.

과제의 해결 수단

[0014] 일 실시 예에 따른 도어락 키 등록방법은, 사용자 단말이 도어락 앱을 실행하는 단계와, 사용자 단말이 사용자 조작에 의해 도어락 키 등록을 위한 사용자 인증정보를 입력 받는 단계와, 사용자 단말이 사용자 인증정보를 암호화하고 암호화된 사용자 인증정보를 보안 서버에 전송하는 단계와, 보안 서버가 사용자 인증정보를 검증하고 검증이 이루어지면 도어락 키를 생성하여 사용자 단말의 보안영역에 주입하는 단계와, 사용자 단말 및 도어락 디바이스 간의 근거리 무선통신을 통해 도어락 디바이스에 도어락 키를 저장하는 단계를 포함한다.

[0015] 사용자 인증정보를 입력 받는 단계에서, 사용자가 사용자 단말을 이용하여 도어락 디바이스에 포함된 QR 코드를 촬영하거나 도어락 디바이스에 기입된 도어락 S/N을 직접 입력하는 방식을 통해 사용자 인증정보를 입력 받을 수 있다.

[0016] 사용자 단말은 일반영역 및 보안영역을 포함하고, 암호화된 사용자 인증정보를 보안 서버에 전송하는 단계는, 일반영역이 보안영역에 S/N 암호화 및 키 생성을 요청하는 단계와, 보안영역에서 앱 공개키 및 앱 개인키를 포함하는 앱 키 쌍을 생성하고 서버 공개키로 앱 공개키 및 도어락 S/N를 암호화하는 단계와, 보안영역이 암호화된 앱 공개키 및 도어락 S/N를 일반영역에 전달하는 단계와, 일반영역이 전달받은 암호화된 앱 공개키 및 도어락 S/N를 보안 서버에 전달하는 단계를 포함할 수 있다.

[0017] 보안 서버는 제어부; 하드웨어 보안 모듈(Hardware Security Module: HSM, 이하 'HSM'이라 칭함); 및 DB; 를 포함하고, 사용자 단말의 보안영역에 주입하는 단계는, 제어부가 사용자 단말로부터 수신된 앱 공개키 및 도어락 S/N의 복호화를 HSM에 요청하는 단계와, HSM이 서버 개인키로 앱 공개키 및 도어락 S/N을 복호화 하여 앱 공개키 및 도어락 S/N을 확인하고 확인된 앱 공개키 및 도어락 S/N을 제어부에 전달하는 단계와, 제어부가 DB에서 도어락 S/N 및 도어락 공개키를 확인하고, 도어락 S/N이 존재하면 HSM에 도어락 키 생성을 요청하는 단계와, HSM이 요청에 따라 도어락 키를 생성하고, 생성된 도어락 키를 도어락 공개키로 암호화하며, 생성된 도어락 키 및 도어락 공개키를 앱 공개키로 암호화하는 단계와, HSM이 암호화된 도어락 키 및 도어락 공개키를 제어부에 전달하는 단계와, 제어부가 암호화된 도어락 키 및 도어락 공개키를 사용자 단말에 주입하는 단계를 포함할 수 있다.

[0018] 다른 실시 예에 따른 도어락 키 사용방법은, 도어락 디바이스가 활성화 모드에 진입하면 미리 설정된 시간 동안 미리 설정된 시간간격으로 근거리 무선통신 스캐닝 및 NFC 폴링을 수행하는 단계와, 도어락 디바이스가 도어락 앱을 통한 사용자 단말의 접근을 감지하는 단계와, 사용자 단말 및 도어락 디바이스 간에 NFC 태깅 또는 근거리 무선통신 페어링 되는 단계와, 인증 데이터 생성 및 검증을 통해 도어락 디바이스가 잠금 해제되는 단계를 포함한다.

[0019] 도어락 디바이스가 잠금 해제되는 단계는, 도어락 디바이스가 사용자 단말에 랜덤 값 생성 및 인증을 요청하는 단계와, 사용자 단말이 랜덤 값을 생성하고 랜덤 값 및 도어락 키로 서명 값을 생성하고, 인증 데이터를 생성하는 단계와, 사용자 단말이 인증 데이터를 도어락 디바이스에 전달하는 단계와, 도어락 디바이스가 수신된 인증 데이터를 도어락 개인키로 복호화 하고, 랜덤 값을 검증하며, 도어락 키를 검증하고 권한을 확인한 후, 검증을 모두 성공하면 인증이 완료되고 도어락 디바이스의 잠금을 해제하는 단계를 포함할 수 있다.

[0020] 인증 데이터를 생성하는 단계에서, 랜덤 값, 도어락 키 및 서명 값을 도어락 공개키로 암호화하여 인증 데이터를 생성할 수 있다.

[0021] 도어락 키 사용방법은, 사용자 단말이 공유자 단말과 도어락 키를 영구, 기간설정 및 1회용으로 구분하여 공유하는 단계와, 사용자 단말이 공유자 단말로부터 공유한 키를 회수하는 단계 중 적어도 하나를 더 포함할 수 있다.

[0022] 다른 실시 예에 따른 출입관리 시스템은, 도어락 키에 의해 잠금 해제되는 도어락 디바이스와, 도어락 앱을 실행하고 도어락 키를 사용하여 NFC 태깅, 근거리 무선통신 및 지문인식 중 적어도 하나를 통해 도어락 디바이스를 잠금 해제하며, 일반영역과는 분리된 보안영역에 도어락 키를 저장하는 사용자 단말과, 사용자 단말을 등록하고 등록된 사용자 단말 내부에 보안영역을 활성화하며 사용자 단말의 요청에 따라 도어락 키를 생성한 후 생성된 도어락 키를 사용자 단말의 활성화된 보안영역에 주입하는 보안 서버를 포함한다.

[0023] 도어락 디바이스는, QR 코드 및 S/N 중 적어도 하나를 포함하는 사용자 인증정보가 기입되고, 근거리 무선통신 등록 버튼 및 지문 등록 버튼을 구비하며, 사용자 단말의 도어락 앱과의 NFC 태깅을 통해 도어락 디바이스를 잠금 해제하는 NFC 리더기와, 사용자 단말의 도어락 앱과의 근거리 무선통신을 통해 도어락 디바이스를 잠금 해제하는 근거리 무선통신 모듈과, 사용자의 지문인식에 의해 도어락 디바이스를 잠금 해제하는 지문인식 센서를 포함할 수 있다.

[0024] 도어락 디바이스는 도어락 디바이스 내 보안 모듈에서 도어락 개인키 및 도어락 공개키를 포함하는 도어락 키 쌍을 생성하고, 도어락 개인키는 보안 모듈 내에 보관하며, 도어락 공개키와 도어락 S/N 쌍을 보안 서버에 전송하고, 보안 서버는 HSM에서 서버 개인키 및 서버 공개키를 포함하는 서버 키 쌍을 생성하고, 서버 개인키는 HSM 내에 보관하며, 서버 공개키를 도어락 디바이스에 주입할 수 있다.

발명의 효과

[0026] 일 실시 예에 따른 도어락 키 등록 및 사용방법과 그 출입관리 시스템에 따르면, 하드웨어 기반의 보안환경과 소프트웨어 기반의 보안환경을 지원하는 사용자 단말을 사용하여 카드 키를 소지하지 않더라도 건물출입시 게이트 출입을 가능하게 할 수 있을 뿐만 아니라, 사용자 편의를 향상시킬 수 있다.

[0027] 사용자 단말이 보안 서버로부터 전달받은 도어락 키를 하드웨어 기반의 보안환경을 제공하는 TEE 보안영역 또는 소프트웨어 기반의 보안환경을 제공하는 WBC 보안영역에 저장함으로써 건물출입용 게이트의 도어락 키에 대한 보안을 향상시킬 수 있는 효과가 있다.

[0028] 도어락 앱이 설치된 사용자 단말을 이용하여 도어락 디바이스를 잠금 해제할 때, NFC 방식, 근거리 무선통신(UWB/BLE), 지문인식 방식 모두를 지원할 수 있어 사용자 편의성을 높일 수 있는 효과가 있다.

[0029] 도어락 앱을 이용하여 도어락 키를 사용하는 경우, 도어락 앱은 일반영역에서 실행되더라도 일반영역을 통해 접근이 불가능한 보안영역에 도어락 키를 별도로 저장할 수 있어 손쉽게 해킹되는 것을 미연에 방지하는 효과가 있다.

도면의 간단한 설명

[0031] 도 1은 본 발명의 실시예에 따른 출입관리 시스템의 구성을 도시한 도면,

도 2는 본 발명의 일 실시 예에 따른 사용자의 도어락 키 등록 시나리오 예를 도시한 도면,

도 3은 본 발명의 일 실시 예에 따른 사용자의 도어락 키 사용 시나리오 예를 도시한 도면,

도 4는 본 발명의 일 실시 예에 따른 도어락 키 공유 시나리오의 예를 도시한 도면,

도 5는 본 발명의 일 실시 예에 따른 공유자의 도어락 키 사용 시나리오의 예를 도시한 도면,

도 6은 본 발명의 일 실시 예에 따른 도어락 키 등록 프로세스를 도시한 도면,

도 7은 본 발명의 일 실시 예에 따른 도어락 키 사용 프로세스를 도시한 도면,

도 8은 본 발명의 일 실시 예에 따른 구성요소 간 상호 보안 인증을 위한 도어락 등록 예를 도시한 도면,

도 9 및 도 10은 본 발명의 일 실시 예에 따른 도어락 키 등록 프로세스를 보다 세부적으로 도시한 도면,

도 11은 본 발명의 일 실시 예에 따른 도어락 키 사용 프로세스를 세부적으로 도시한 도면,

도 12는 본 발명의 일 실시 예에 따른 인증 데이터를 구조를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0032] 이상의 본 발명의 목적들, 다른 목적들, 특징들 및 이점들은 첨부된 도면과 관련된 이하의 바람직한 실시 예들을 통해서 쉽게 이해될 것이다. 그러나 본 발명은 여기서 설명되는 실시 예들에 한정되지 않고 다른 형태로 구체화될 수도 있다. 오히려, 여기서 소개되는 실시 예들은 개시된 내용이 철저하고 완전해질 수 있도록 그리고 당업자에게 본 발명의 사상이 충분히 전달될 수 있도록 하기 위해 제공되는 것이다.

[0033] 본 명세서에서, 어떤 구성요소가 다른 구성요소 상에 있다고 언급되는 경우에 그것은 다른 구성요소 상에 직접 형성될 수 있거나 또는 그들 사이에 제3의 구성요소가 개재될 수도 있다는 것을 의미한다.

[0034] 본 명세서에서 제1, 제2 등의 용어가 구성요소들을 기술하기 위해서 사용된 경우, 이들 구성요소들이 이 같은 용어들에 의해서 한정되어서는 안 된다. 이들 용어들은 단지 어느 구성요소를 다른 구성요소와 구별시키기 위해서 사용되었을 뿐이다. 여기에 설명되고 예시되는 실시 예들은 그것의 상보적인 실시 예들도 포함한다.

[0035] 또한, 제1 엘리먼트 (또는 구성요소)가 제2 엘리먼트(또는 구성요소) 상(ON)에서 동작 또는 실행된다고 언급될 때, 제1 엘리먼트(또는 구성요소)는 제2 엘리먼트(또는 구성요소)가 동작 또는 실행되는 환경에서 동작 또는 실행되거나 또는 제2 엘리먼트(또는 구성요소)와 직접 또는 간접적으로 상호 작용을 통해서 동작 또는 실행되는 것으로 이해되어야 할 것이다.

[0036] 어떤 엘리먼트, 구성요소, 장치, 또는 시스템이 프로그램 또는 소프트웨어로 이루어진 구성요소를 포함한다고 언급되는 경우, 명시적인 언급이 없더라도, 그 엘리먼트, 구성요소, 장치, 또는 시스템은 그 프로그램 또는 소프트웨어가 실행 또는 동작하는데 필요한 하드웨어(예를 들면, 메모리, CPU 등)나 다른 프로그램 또는 소프트웨어(예를 들면 운영체제나 하드웨어를 구동하는데 필요한 드라이버 등)를 포함하는 것으로 이해되어야 할 것이다.

[0037] 또한, 어떤 엘리먼트(또는 구성요소)가 구현됨에 있어서 특별한 언급이 없다면, 그 엘리먼트(또는 구성요소)는 소프트웨어, 하드웨어, 또는 소프트웨어 및 하드웨어 어떤 형태로도 구현될 수 있는 것으로 이해되어야 할 것이다.

[0038] 또한, 본 명세서에서 사용된 용어는 실시 예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 '포함한다(comprises)' 및/또는 '포함하는(comprising)'은 언급된 구성요소는 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다.

[0039] 이하, 아래의 특정 실시 예들을 기술하는데 있어서, 여러 가지의 특정적인 내용들은 발명을 더 구체적으로 설명하고 이해를 돕기 위해 작성되었다. 하지만 본 발명을 이해할 수 있을 정도로 이 분야의 지식을 갖고 있는 독자는 이러한 여러 가지의 특정적인 내용들이 없어도 사용될 수 있다는 것을 인지할 수 있다.

[0040] 어떤 경우에는, 발명을 기술하는 데 있어서 흔히 알려졌으면서 발명과 크게 관련 없는 부분들은 본 발명을 설명하는 데 있어 별 이유 없이 혼돈이 오는 것을 막기 위해 기술하지 않음을 미리 언급해 둔다.

[0041] 이하, 본 명세서의 실시 예를 첨부된 도면을 참조하여 설명한다. 본 명세서에 따른 동작 및 작용을 이해하는 데 필요한 부분을 중심으로 상세히 설명한다. 본 명세서의 실시 예를 설명하면서, 본 명세서가 속하는 기술 분야에 익히 알려졌고 본 명세서와 직접적으로 관련이 없는 기술 내용에 대해서는 설명을 생략한다. 이는 불필요한 설명을 생략함으로써 본 명세서의 요지를 흐리지 않고 더욱 명확히 전달하기 위함이다.

[0042] 또한, 본 명세서의 구성 요소를 설명하는 데 있어서, 동일한 명칭의 구성 요소에 대하여 도면에 따라 다른 참조부호를 부여할 수도 있으며, 서로 다른 도면임에도 동일한 참조부호를 부여할 수도 있다. 그러나 이와 같은 경우라 하더라도 해당 구성 요소가 실시 예에 따라 서로 다른 기능을 갖는다는 것을 의미하거나, 서로 다른 실시 예에서 동일한 기능을 갖는다는 것을 의미하는 것은 아니며, 각각의 구성 요소의 기능은 해당 실시 예에서의 각각의 구성 요소에 대한 설명에 기초하여 판단하여야 할 것이다.

[0043] 본 명세서에서 각각의 구성들은 기능 및/또는 논리적으로 분리될 수 있음을 나타내는 것이며, 반드시 각각의 구성이 별도의 물리적 장치로 구분되거나 별도의 코드로 작성됨을 의미하는 것은 아님을 본 발명의 기술분야의 평균적 전문가는 용이하게 추론할 수 있을 것이다.

[0044] 또한, 본 명세서에서 각각의 구성들은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 소정의 코드와 소정의 코드가 수행되기

위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것이 아님은 본 발명의 기술분야의 평균적 전문가에게는 용이하게 추론될 수 있다.

[0045] 도 1은 본 발명의 실시예에 따른 출입관리 시스템의 구성을 도시한 도면이다.

[0046] 도 1을 참조하면, 출입관리 시스템(1)은 도어락 디바이스(10), 사용자 단말(12) 및 보안 서버(14)를 포함한다.

[0047] 출입관리 시스템(1)은 이동통신 기술의 발달로 널리 사용되는 스마트폰과 같은 사용자 단말(12)에 도어락 앱(Door-lock App)을 설치하고, 출입 게이트에 설치된 도어락 디바이스(10)를 비접촉방식으로 잠금 해제할 수 있는 도어락 키(Door-lock key)를 일반영역과 하드웨어 또는 소프트웨어적으로 분리된 보안영역에 구비함으로써, 카드 키 없이도 건물에 설치된 보안 게이트를 출입할 수 있어 사용자 편의를 증가시킬 수 있다. 도어락 키는 디지털 키(Digital key) 또는 스마트 키(Smart key)로서, 도어락 디바이스(10)가 별도의 키 패드 없이도 도어락 키를 이용하여 도어락 디바이스(10)를 잠금 해제할 수 있다.

[0048] 도어락 디바이스(10)는 사용자 단말(12)에 발급된 도어락 키로 실제 잠금 및 해제를 수행하는 기기이다. 보안 서버(14)에 등록하여 도어락 키를 발급받는다.

[0049] 사용자 단말(12)은 보안 서버(14)에 등록하여 디지털 키를 발급받고, 발급받은 도어락 키를 사용, 공유 및 삭제하는 기능을 가지며, 보안요소를 통하여 중요한 정보와 로직을 보호한다. 사용자 단말(12)은 잠금을 사용자 단말(12)의 도어락 앱의 보안영역에 저장된 도어락 키를 통하여 도어락 디바이스(10)의 잠금을 해제한다.

[0050] 사용자 단말(12)은 도어락 디바이스(10)와 근거리 무선통신이 가능한 휴대용 단말 장치로써, 스마트 폰, 테블릿 PC, 웨어러블 디바이스와 같은 전자장치가 될 수 있다. 사용자 단말(12)에는 도어락 앱이 설치된다. 도어락 앱을 이용하여 출입자 등록을 신청할 수 있다. 이 경우, 사용자 단말(12)은 휴대 가능한 모바일 단말일 필요는 없고, 건물출입 허가를 신청하기 위하여 웹 브라우저를 지원하는 PC일 수도 있다.

[0051] 사용자 단말(12)은 일반영역과 보안영역으로 운영되면서, 일반영역에 보안용 어플리케이션으로 동작하는 도어락 앱이 설치되고, 도어락 앱을 통해 일반영역과 보안영역을 연동시킬 수 있으며, 보안 서버(14)로부터 주입된 도어락 키를 도어락 앱의 보안영역에 저장할 수 있다. 보안영역은 도어락 키 보관 및 암호화 등을 수행하며, 일반영역은 UI, 네트워킹 기능 등을 수행한다.

[0052] 사용자 단말(12)은 일반 운영체제와 보안 운영체제로 운영되며, 도어락 앱을 가지고 보안 서버(14)를 통해 출입자 본인인증을 거치고, 보안 서버(14)로부터 인증이 완료되면 암호화된 도어락 키를 보안영역에서 복호화 하여 저장할 수 있다.

[0053] 사용자 단말(12)은 하드웨어 기반의 TEE(Trusted Execution Environment) 보안기술 및 소프트웨어 기반 WBC(White Box Cryptography) 보안기술 중 하나 이상의 보안기술이 적용될 수 있다. TEE 보안기술은 일반영역과 보안영역이 물리적으로 분리된 ARM 트러스트존 기반의 하드웨어 보안환경을 지원하는 보안기술이다. WBC 보안기술은 일반영역의 중요한 데이터 정보를 암호화 알고리즘을 통해 분산하고 난독화 함으로서 보안영역을 생성하는 보안기술이다.

[0054] 보안 서버(14)는 도어락 디바이스(10)와 사용자 단말(12)의 도어락 키를 발급, 공유 및 원격 삭제한다. 예를 들어, 보안 서버(14)는 사용자 단말(12)을 등록하고 등록된 사용자 단말(12) 내부에 보안영역을 활성화한다. 이어서, 보안 서버(14)는 사용자 단말(12)의 요청에 따라 도어락 키를 생성하고 생성된 도어락 키를 사용자 단말(12)의 활성화된 보안영역에 주입한다.

[0055] 보안 서버(14)는 사용자 단말(12)이 도어락 앱을 통해 접속되면 건물출입허가를 신청하기 위한 출입자 정보 입력메뉴 및 개인정보 입력메뉴를 제공하며, 출입자 정보에 대응되는 도어락 키를 생성하여 저장할 수 있다.

[0056] 보안 서버(14)는 도어락 디바이스(10)를 잠금 해제할 수 있는 도어락 키를 출입자 정보에 대응되어 매핑 테이블로 저장할 수 있으며, 도어락 키와 출입자 정보를 DB화하여 저장할 수 있다. 보안 서버(14)는 사용자 단말(12)을 통해 입력되는 개인정보를 이용하여 출입자의 본인 인증 과정을 수행할 수 있다.

[0057] 보안 서버(14)는 사용자 단말(12)에서 도어락 디바이스(10)의 동작을 제어(예를 들어, 도어락 디바이스의 잠금 해제)하기 위한 도어락 키를 생성하여 도어락 디바이스(12) 및 사용자 단말(12)로 할당하는 서버가 될 수 있다.

[0058] 예를 들어, 최초 사용자 단말(12)이 도어락 디바이스(12)에 등록되면, 사용자 단말(12)은 보안 서버(14)에 도어락 키 할당을 요청한다. 이에 따라, 보안 서버(14)는 도어락 키를 생성하여 사용자 단말(12)로 전송한다. 사용자 단말(12)은 보안 서버(14)로부터 수신한 도어락 키를 도어락 디바이스(12)로 전송하고, 도어락 키를 사용자

단말(12)의 보안 영역 내에 저장할 수 있다.

[0059] 도 2는 본 발명의 일 실시 예에 따른 사용자의 도어락 키 등록 시나리오 예를 도시한 도면이다.

[0060] 도 2를 참조하면, 준비 단계(210)에서, 사용자가 도어락 디바이스(10)를 구매한다. 도어락 디바이스(10)에는 NFC 리더기(Reader), 근거리 무선통신 모듈, 지문인식 센서가 포함될 수 있으며, 별도의 키 패드가 필요 없다. 근거리 무선통신 모듈은 초광대역(UWB), 블루투스(BLE), 와이파이(Wi-Fi) 기능 등을 지원할 수 있다. 그리고 사용자는 사용자 단말(12)의 도어락 앱을 다운로드한 후 회원가입 한다.

[0061] 이어서, 사용자는 등록 절차(220)를 수행한다. 이를 위해, 도어락 디바이스(10)의 소정 부분, 예를 들어, 도어락 디바이스의 안쪽에는 등록을 위한 사용자 인증정보(예를 들어, QR 코드 및 시리얼 넘버(S/N: Serial No, 이하 'S/N'라 칭함))가 생산 시 기입되어 있다. 또한, 근거리 무선통신 등록 버튼, 지문 등록 버튼 등이 포함될 수 있다. 도 2에서는 사용자가 도어락 디바이스(10)의 커버를 분리한 후 안쪽에 등록을 위한 정보 또는 버튼을 이용하고 있으나, 이는 본 발명의 이해를 돕기 위한 일 실시 예일뿐, 이에 한정되는 것은 아니다.

[0062] 사용자는 도어락 앱을 실행하여 도어락 디바이스의 QR 코드를 촬영하거나 도어락 S/N을 직접 입력하여 도어락 디바이스를 도어락 앱에 등록한다. UWB 기능을 사용하기 위해서 사용자가 도어락 디바이스(10)의 블루투스 등록 버튼을 눌러 스마트폰과 페어링 할 수 있다. 지문을 등록하기 위해서 사용자가 도어락 디바이스(10)의 지문등록 버튼을 눌러 지문을 등록할 수 있다. 등록 시, 도어락 앱에서 등록한 QR 코드 또는 S/N를 보안 서버가 검증하는 단계가 수반된다.

[0063] 등록 절차가 완료되면, 사용자가 도어락 앱을 이용하여 도어락 디바이스(10)를 사용 가능한 상태가 된다(230).

[0064] 도 3은 본 발명의 일 실시 예에 따른 사용자의 도어락 키 사용 시나리오 예를 도시한 도면이다.

[0065] 도 3을 참조하면, 도어락 사용 예는 (a)NFC 사용, (b)UWB(BLE) 사용, (c)지문 사용 등이 있다.

[0066] (a)NFC 기능을 사용하는 경우, 사용자는 사용자 단말(12)을 도어락 디바이스(10)에 NFC 태깅(tagging) 하여 사용한다.

[0067] (b)UWB(BLE) 기능을 사용하기 위해, 사용자는 사용자 단말(12)의 도어락 앱에서 도어락 디바이스(10)와의 거리를 미리 설정할 수 있으며, 사용자 단말(12)과 도어락 디바이스(10)가 미리 설정된 거리 이내에 진입하면, 도어락 디바이스(10)가 작동한다.

[0068] (c)지문 기능을 사용하는 경우, 사용자가 자신의 지문으로 도어락 디바이스(10)의 지문인식센서에 터치 시 도어락 디바이스(10)가 작동한다.

[0069] 도 4는 본 발명의 일 실시 예에 따른 도어락 키 공유 시나리오의 예를 도시한 도면이다.

[0070] 도 4를 참조하면, 사용자는 공유자와 도어락 키를 공유할 수 있다(S410). 이때, 사용자 단말(12)은 다른 사용자 단말인 공유자 단말(11)과 도어락 키를 영구/기간설정/1회용 등으로 구분하여 공유할 수 있다. 또한 사용자 단말(12)은 공유자 단말(11)로부터 공유한 키를 즉시 회수할 수 있다(S420).

[0071] 도 5는 본 발명의 일 실시 예에 따른 공유자의 도어락 키 사용 시나리오의 예를 도시한 도면이다.

[0072] 도 5를 참조하면, 공유자의 지문은 도어락 디바이스(10)에 등록이 되어 있지 않으므로, NFC 또는 UWB(BLE) 기능을 이용하여 등록 기능을 활성화한 이후 공유자의 지문 등록을 완료한다. 지문을 등록한 이후, 공유자는 도어락 디바이스(10)의 지문인식센서에 터치하여 도어락 디바이스(10)를 잠금 해제할 수 있다.

[0073] 도 6은 본 발명의 일 실시 예에 따른 도어락 키 등록 프로세스를 도시한 도면이다.

[0074] 도 6을 참조하면, 사용자 단말(12)은 사용자에 의해 도어락 앱을 실행하여 회원가입 및 로그인 절차를 완료한다(S601).

[0075] 이어서, 사용자의 소정의 동작, 예를 들어, 도어락 디바이스(10)의 뒷면을 탈락하는 동작(S602)을 거친 후, 사용자 단말(12)을 통해 도어락 메뉴 등록을 시작한다(S603).

[0076] 사용자 단말(12)은 도어락 디바이스(10)에 포함된 시리얼 번호를 확인한 사용자에 의해 S/N를 입력 받거나, 도어락 디바이스(10)에 포함된 QR 코드를 촬영하는 동작을 통해 NFC 등록을 완료하고 NFC 기능을 사용할 수 있게 된다(S604).

[0077] 이어서, 사용자 단말(12)은 인증서를 생성(S605) 하고, 인증서를 보안 서버(14)에 전송한다(S606). 보안 서버

(14)는 판매정보를 확인(S607) 하고, 도어락 키를 사용자 단말(12)에 전달한다(S608).

[0078] 이어서, 사용자의 사용자 단말(12) 및 도어락 디바이스(10) 간의 블루투스 연결 동작을 통해 페어링 된다. 예를 들어, 사용자가 사용자 단말(12)의 블루투스 등록 버튼을 누르고(S609), 도어락 디바이스(10)의 블루투스 등록 버튼을 누름으로써(S610), 사용자 단말(12) 및 도어락 디바이스(10) 간에 블루투스 페어링 된다(S611).

[0079] 도 7은 본 발명의 일 실시 예에 따른 도어락 키 사용 프로세스를 도시한 도면이다.

[0080] 도 7을 참조하면, NFC 기능을 사용하는 경우, 사용자는 사용자 단말(12)을 도어락 디바이스(10)에 NFC 태깅한다(701). 이때, 사용자 단말(12)은 도어락 사용자 정보를 보안 서버(14)에 전송함에 따라 보안 서버(14)는 도어락 사용자 정보를 수집한다(S702).

[0081] 다른 예로, UWB(BLE) 기능을 사용하는 경우, 사용자가 사용자 단말(12)의 도어락 앱을 통해 도어락 디바이스(10)와의 거리를 설정(S703) 하면, 사용자 단말(12)이 도어락 디바이스(10)와 미리 설정된 거리 이내에 진입할 때 도어락 디바이스(10)를 잠금 해제한다(S704).

[0082] 도 8은 본 발명의 일 실시 예에 따른 구성요소 간 상호 보안 인증을 위한 도어락 등록 예를 도시한 도면이다.

[0083] 도 8을 참조하면, 도 8의 (a)에 도시된 바와 같이, 도어락 디바이스(10)는 도어락 디바이스 내 보안 모듈에서 도어락 개인키(Door Pri.) 및 도어락 공개키(Door Pub.)를 포함하는 도어락 키 쌍(Door Key Pair)을 생성하고, 도어락 개인키는 보안 모듈 내에 보관하며, 도어락 공개키와 도어락 S/N(Serial Number) 쌍을 보안 서버(14)에 전송한다. QR 코드에는 S/N가 저장된다. 도어락 키 쌍 생성 시 S/N를 Seed로 하여 중복확률을 제거할 수 있다.

[0084] 도 8의 (b)를 참조하면, 보안 서버(14)는 HSM(Hardware security module)에서 서버 개인키(Server Pri.) 및 서버 공개키(Server Pub.)를 포함하는 서버 키 쌍을 생성한다. 서버 개인키는 HSM 내에 보관하고, 서버 공개키는 모든 도어락 디바이스에 공통으로 주입한다. 도어락 앱 개발 시(Build 시)에 보안영역에 서버 공개키가 저장된다.

[0085] 도 8의 (c)를 참조하면, 도어락 디바이스(10)는 도어락 S/N(Serial Number) 및 도어락 공개키 쌍(S/N + 도어락 공개키)을 보안 서버(14)에 전송한다. 보안 서버(14)는 도어락 S/N과 도어락 공개키를 매핑한 매핑 테이블을 저장할 수 있다.

[0086] 도 9 및 도 10은 본 발명의 일 실시 예에 따른 도어락 키 등록 프로세스를 보다 세부적으로 도시한 도면이다.

[0087] 도 9 및 도 10을 참조하면, 사용자 단말(12)은 보안영역(121) 및 일반영역(122)이 분리되어 있다. 보안영역(121)은 TEE/USIM/eSIM/WBC 등이 있다. 예를 들어, 도어락 키 앱이 설치된 사용자 단말(12)을 이용하여 보안 서버(14)로부터 전달받은 도어락 키를 하드웨어 기반의 보안환경을 제공하는 TEE 보안영역과 소프트웨어 기반의 보안환경을 제공하는 WBC 보안영역에 저장함으로써 건물출입용 게이트의 도어락 키에 대한 보안을 향상시킨다. 또한, 보안 서버(14)는 제어부(141), 하드웨어 보안 모듈(Hardware security module: HSM, 이하, 'HSM'이라 칭함)(142), DB(143)를 포함한다.

[0088] 사용자 단말(12)은 일반영역(122)에서 도어락 키 앱을 설치 및 실행하고 회원가입 및 로그인을 완료한 후, 도어락 키 앱을 최초 실행하여 도어락 등록을 선택한다(S901). 이때, 보안 서버(14)의 제어부(141)는 가입된 회원정보를 DB(143)에 저장한다(S902).

[0089] 이어서, 도어락 디바이스(10)는 사용자 조작에 의해 도어락 키 등록요청을 입력 받는다. 예를 들어, 사용자가 도어락 디바이스(10)의 뒷면을 탈착한 후 도어락 키 등록 버튼을 선택한다(S903). 도어락 키 등록요청이 입력되면 도어락 디바이스(10)는 미리 설정된 시간(예를 들어, 5분) 동안 통신 대기 상태 모드를 유지(S904) 하면서 설정된 시간 단위(예를 들어, 1초)로 근거리 무선통신을 위한 NFC 폴링(polling) 및 BLE 스캔을 진행한다(S913).

[0090] 사용자 단말(12)은 사용자 조작에 의해 사용자 인증정보를 입력 받는다(S905). 예를 들어, 사용자 인증정보가 QR 코드이면, 카메라를 이용하여 촬영된 영상정보를 통해 사용자 인증정보를 입력 받을 수 있으며, 사용자 인증정보가 도어락 S/N이면, 사용자로부터 도어락 S/N을 직접 입력 받을 수 있다.

[0091] 이후 절차는 사용자 단말(12)이 사용자 인증정보를 암호화하여 보안 서버(14)에 전달하는 단계이다.

[0092] 사용자 인증정보가 입력되면, 사용자 단말(12)의 일반영역(122)은 보안영역(121)에 S/N 암호화 및 키 생성을 요청한다(S906). 그러면, 보안영역(121)은 앱 공개키 및 앱 개인키를 포함하는 앱 키 쌍을 생성하고 서버 공개키

로 앱 공개키 및 도어락 S/N를 암호화한다(S907). 이어서, 보안영역(121)은 암호화된 앱 공개키 및 도어락 S/N을 일반영역(122)에 전달(S908) 하고, 일반영역(122)은 전달받은 암호화된 앱 공개키 및 도어락 S/N을 보안 서버(14)의 제어부(141)에 전달한다(S909).

[0093] 이후 절차는 보안 서버(14)가 사용자 단말(12)로부터 전달된 사용자 인증정보를 검증하는 단계이다.

[0094] 보안 서버(14)의 제어부(141)는 HSM(142)에 복호화를 요청(S910)하고, HSM(142)은 서버 개인키로 앱 공개키 및 도어락 S/N을 복호화 하여 앱 공개키 및 도어락 S/N을 확인한다(S911). 그리고 HSM(142)은 확인된 앱 공개키 및 도어락 S/N을 제어부(141)에 전달한다(S912).

[0095] 보안 서버(14)의 제어부(141)는 DB(143)에서 도어락 S/N 및 도어락 공개키를 확인한다(S920). 이때, 도어락 S/N이 존재하는지 여부를 판단(S921) 하고, 도어락 S/N이 미존재 하면, 사용자 단말(12)의 일반영역(122)은 미등록 도어락 안내 팝업 후 도어락 키 앱을 종료한다(S922). 이에 비해, 도어락 S/N이 존재하면, 보안 서버(14)의 제어부(141)는 HSM(142)에 도어락 키 생성을 요청한다(S923). 요청에 따라, 보안 서버(14)의 HSM(142)은 도어락 키를 생성하고, 생성된 도어락 키를 도어락 공개키로 암호화하며, 생성된 도어락 키 및 도어락 공개키를 앱 공개키로 암호화한다(S924). 이어서, 보안 서버(14)의 HSM(142)은 암호화된 도어락용 도어락 키 및 암호화된 앱용 도어락 공개키를 제어부(141)에 전달한다(S925).

[0096] 이후 절차는 보안 서버(14)가 사용자 단말(12)에 도어락 키를 주입하는 단계이다.

[0097] 보안 서버(14)의 제어부(141)는 앱 공개키로 암호화된 도어락 키 및 도어락 공개키를 사용자 단말(12)의 일반영역(122)으로 전달(S926) 하고, 사용자 단말(12)의 일반영역(122)은 이를 보안영역(121)에 전달한다(S927). 사용자 단말(12)의 보안영역(121)은 앱 개인키로 디지털키를 복호화 하여 저장한다(S928).

[0098] 이후 절차는 사용자 단말(12)과 도어락 디바이스(10) 간의 근거리 무선통신(NFC 또는 BLE)을 통해 도어락 디바이스(10)에 도어락 키를 저장하는 단계이다.

[0099] 도어락 디바이스(10)가 미리 설정된 시간(예를 들어, 1초) 단위로 NFC 폴링 및 BLE 스캔을 수행(S913) 하는 도중에, 사용자 단말(12)의 일반영역(122)은 도어락 공개키로 암호화된 도어락 키를 근거리 무선통신(NFC, BLE 등)을 통해 도어락 디바이스(10)에 전달한다(S929). 도어락 디바이스(10)는 미리 설정된 시간(예를 들어, 5분)이 초과되지 않으면(S930), 도어락 개인키로 암호화된 도어락 키를 복호화 한 후 저장한다(S932). 이에 비해, 미리 설정된 시간을 초과하면(Time Out)(S930), 사용자 단말(12)의 일반영역(122)은 사용자 조작에 의해 도어락 뒷면 등록 버튼 재 선택 후 근거리 무선통신을 재시도할 수 있다(S931).

[0100] 도 11은 본 발명의 일 실시 예에 따른 도어락 키 사용 프로세스를 세부적으로 도시한 도면이다.

[0101] 도 11을 참조하면, 도어락 디바이스(10)는 문 잠김 이후 미리 설정된 시간(예를 들어, 10분) 동안 미리 설정된 시간간격(예를 들어, 1초 간격)으로 근거리 무선통신(BLE/UWB) 스캐닝 및 NFC 폴링(pooling)을 수행하는 활성화 모드(Active Mode)에 진입한다. 이어서, 미리 설정된 시간(예를 들어, 10분) 이후부터는 배터리 절약을 위해 슬립 모드(Sleep Mode)로 진입한다(S1101).

[0102] 활성화 모드에 진입하면, 도어락 디바이스(10)는 미리 설정된 시간간격(예를 들어, 1초 간격)으로 근거리 무선통신(BLE/UWB) 스캔 및 NFC 폴링을 수행하고, 도어락 앱을 통한 사용자 단말(12)의 접근을 감지한다(S1102). 이때, 사용자 단말(12)은 도어락 디바이스(10)와 근거리 무선통신(BLE, UWB) 페어링 되거나 도어락 디바이스(10)에 NFC 태깅된다(S1103).

[0103] 이어서, 도어락 디바이스(10)는 사용자 단말(12)에 랜덤(Random) 값 생성 및 인증을 요청한다(S1104). 사용자 단말(12)은 보안영역(121)에서 랜덤 값을 생성(S1105) 하고 이를 일반영역(122)에 전송한다(S1106).

[0104] 이어서, 일반영역(122)은 랜덤 값 + 도어락 키로 서명 값을 생성하고, (랜덤 값 + 도어락 키 + 서명 값)을 도어락 공개키로 암호화하여 인증 데이터를 생성한다 (S1107). 이어서, 일반영역(122)은 암호화된 인증 데이터를 보안영역(121)에 전달(S1108) 하고, 보안영역(121)은 암호화된 인증 데이터를 도어락 디바이스(10)에 전달한다(S1109).

[0105] 이어서, 도어락 디바이스(10)는 도어락 개인키로 수신된 인증 데이터를 복호화 하고, 랜덤 값을 검증하며, 도어락 키를 검증하고 권한을 확인한 후, 검증을 모두 성공하면 인증이 완료되고 도어락 디바이스(10)의 잠금을 해제한다(S1110). 검증을 실패하면 경고 메시지를 출력한다. 예를 들어, 실패 시, 붉은 색 램프를 표시하고 경고를 표시한다. 미리 설정된 횟수(예를 들어, 5회) 연속 실패 시, 미리 설정된 기간(예를 들어, 5분간) 강제로 슬

립 모드로 전환된다.

[0106] 도어락 상태가 슬립 모드에 진입한 경우에는 사용자가 도어락 화면을 터치하여 근거리 통신 모듈을 활성화(S1111) 시켜 활성화 모드로 전환한다.

[0107] 도 12는 본 발명의 일 실시 예에 따른 인증 데이터를 구조를 도시한 도면이다.

[0108] 도 12를 참조하면, 인증 데이터는 랜덤 값, 도어락 키 및 서명을 포함한다.

[0109] 랜덤 값은 숫자 16개(16byte)로 구성되며, 예를 들어, 0123456789012345 값을 가진다.

[0110] 도어락 키는 사용기간 및 스트링 정보(String)를 포함한다. 사용기간은YYYYMMDDhhmmdd 형태를 가진다. 예를 들어, 20211231120000 (2021년 12월 31일 12시 정각까지 사용 가능), 00000000000000 (사용기간 무제한) 형태를 가진다.

[0111] RSA 2048 사용 시, (랜덤 값 + 디지털 키)를 개인키로 서명하여 서명 데이터를 생성한다.

[0112] 이제까지 본 발명에 대하여 그 실시 예들을 중심으로 살펴보았다. 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시 예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

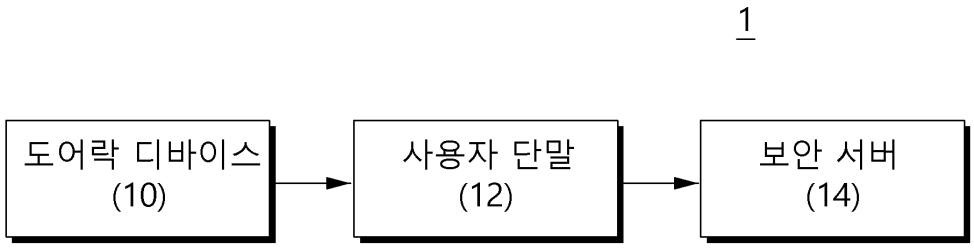
[0114] 10 : 도어락 디바이스

12 : 사용자 단말

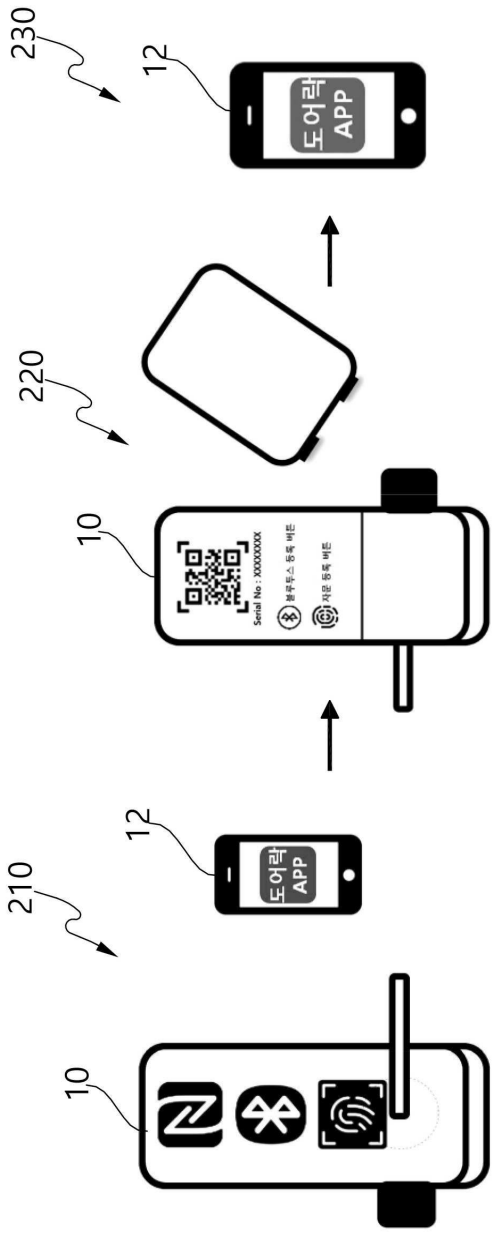
14 : 보안서버

도면

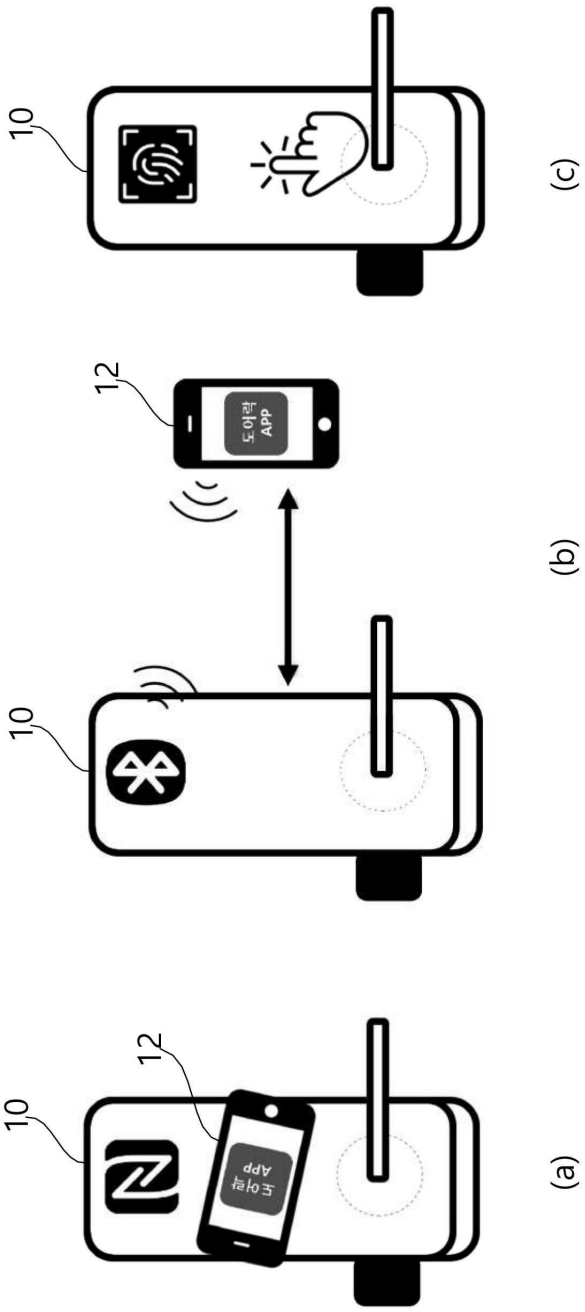
도면1



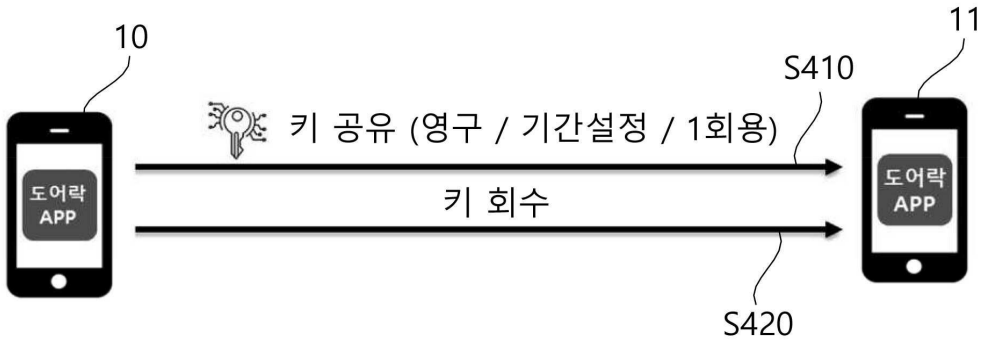
도면2



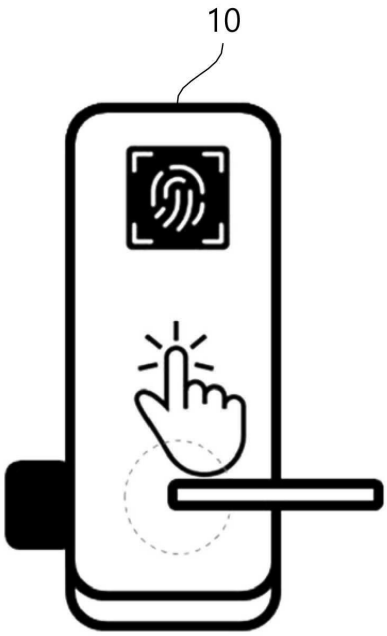
도면3



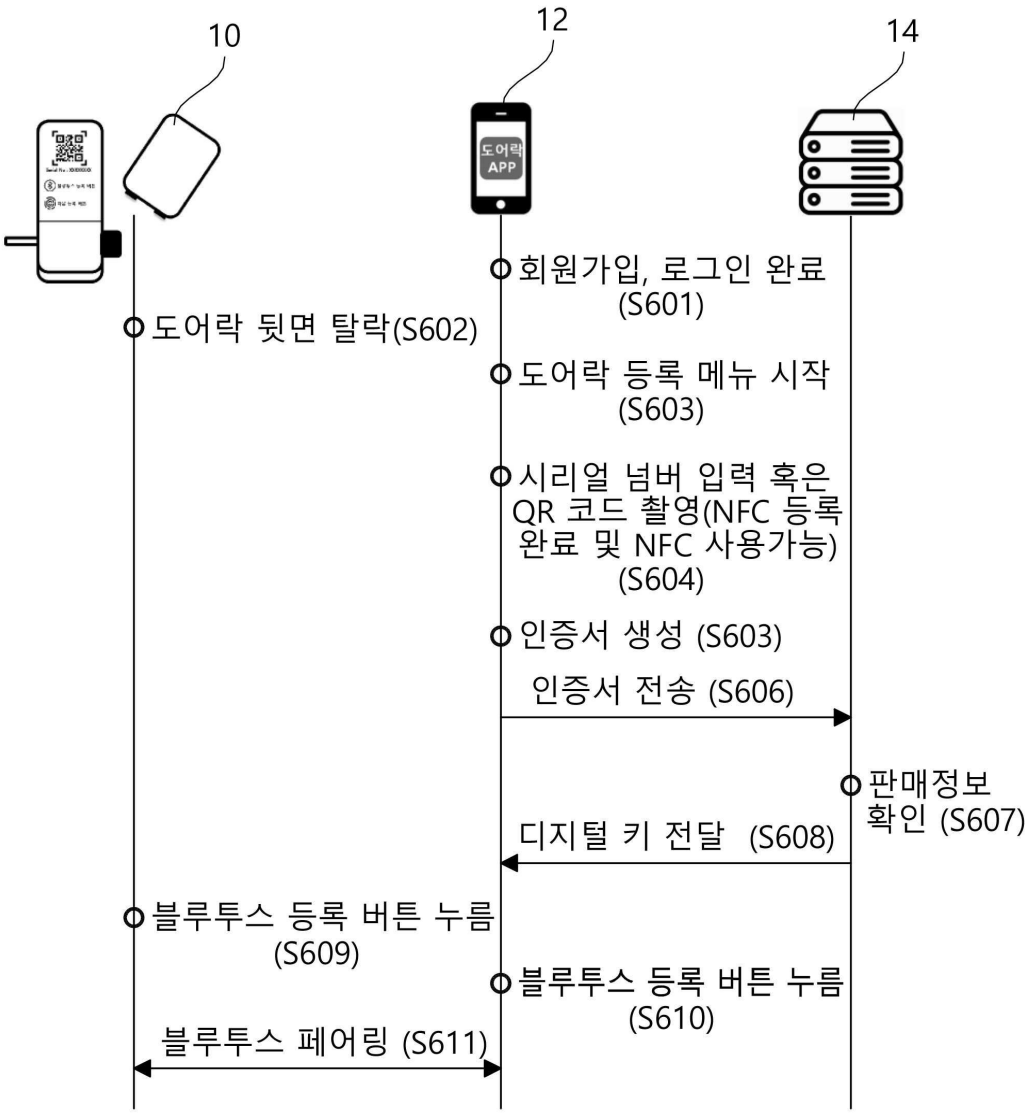
도면4



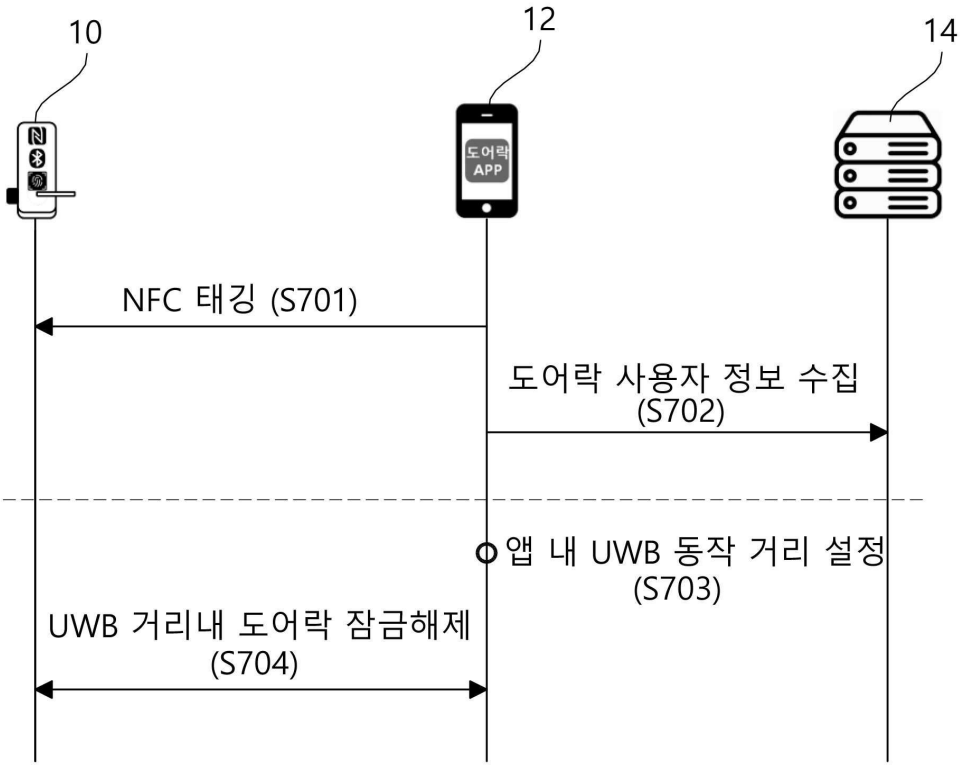
도면5



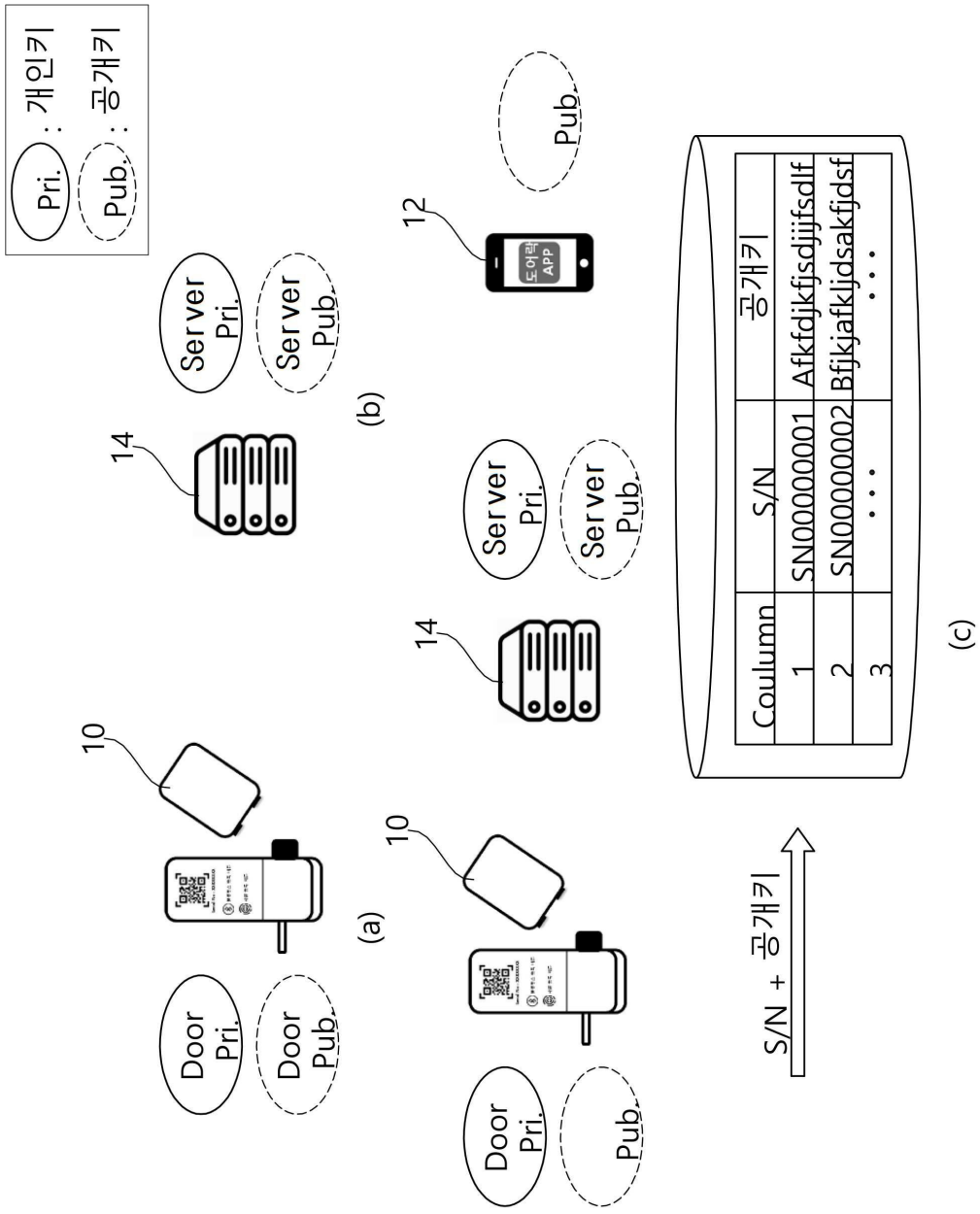
도면6


10
12
14
도어락 APP
회원가입, 로그인 완료 (S601)
도어락 뒷면 탈락(S602)
도어락 등록 메뉴 시작 (S603)
시리얼 넘버 입력 혹은 QR 코드 촬영(NFC 등록 완료 및 NFC 사용가능) (S604)
인증서 생성 (S603)
인증서 전송 (S606)
판매정보 확인 (S607)
디지털 키 전달 (S608)
블루투스 등록 버튼 누름 (S609)
블루투스 등록 버튼 누름 (S610)
블루투스 페어링 (S611)

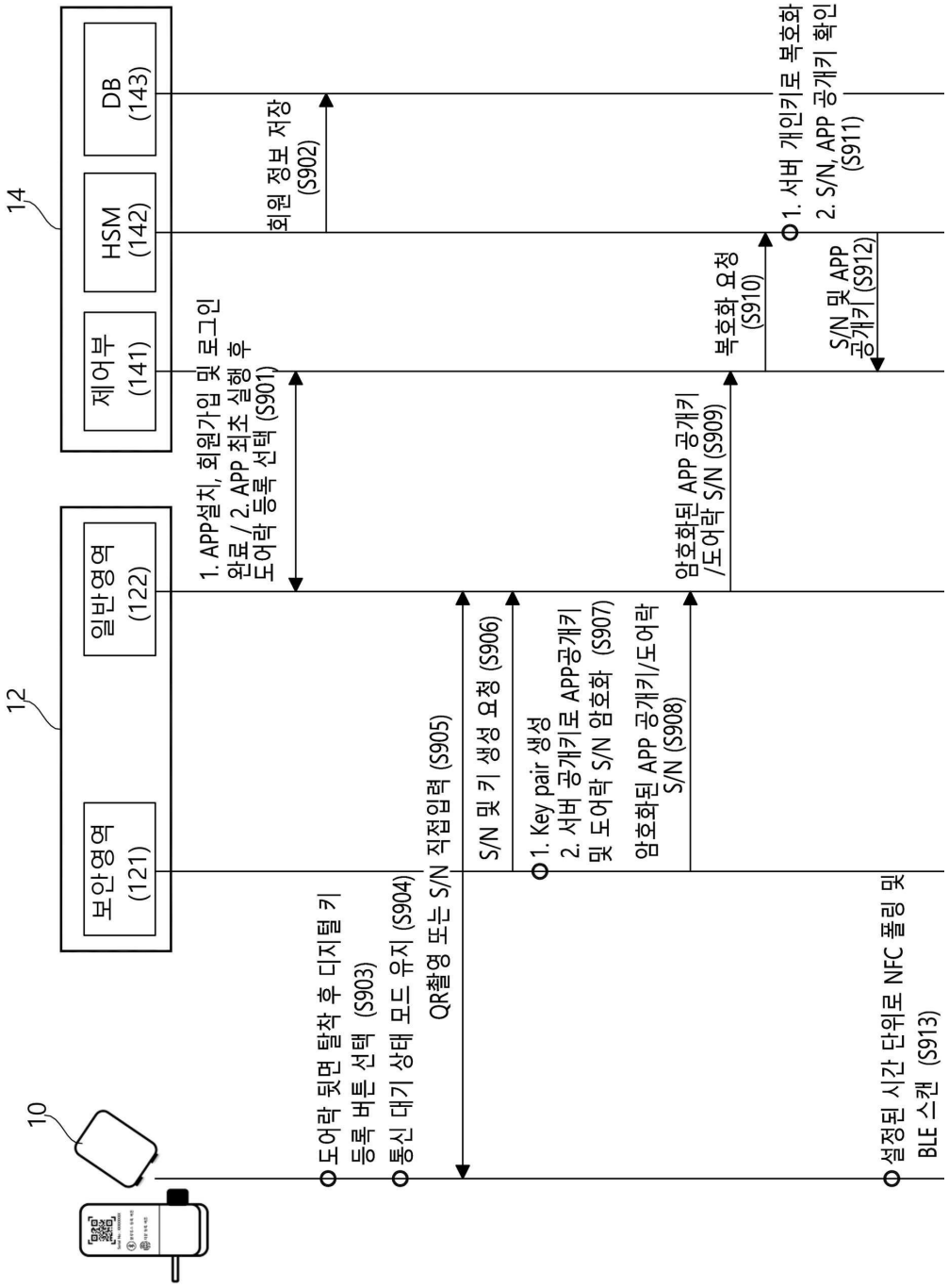
도면7


10
12
14
도어락 APP
NFC 태깅 (S701)
도어락 사용자 정보 수집
(S702)
앱 내 UWB 동작 거리 설정
(S703)
UWB 거리내 도어락 잠금해제
(S704)

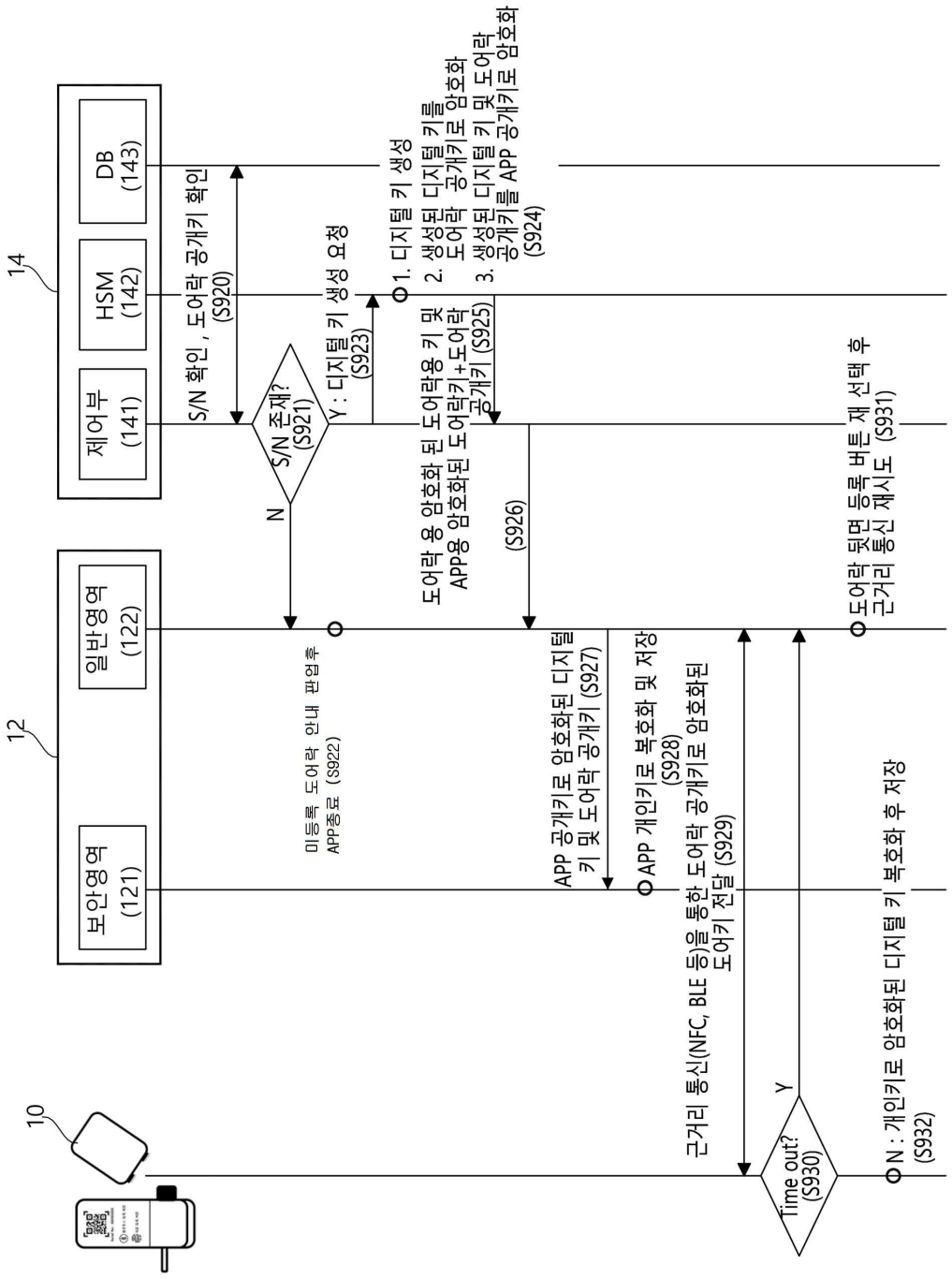
도면8


Pri. : 개인키
Pub. : 공개키
Server Pri.
Server Pub.
14
(b)
12
도어락 APP
Pub.
Server Pri.
Server Pub.
14
10
Door Pri.
Door Pub.
(a)
10
Door Pri.
Pub.
S/N + 공개키
Coulumn
S/N
공개키
1
SN00000001
Afkfdjkfjsdjjifsdlf
2
SN00000002
Bfjkjafkljdsakfjdsf
3
(c)

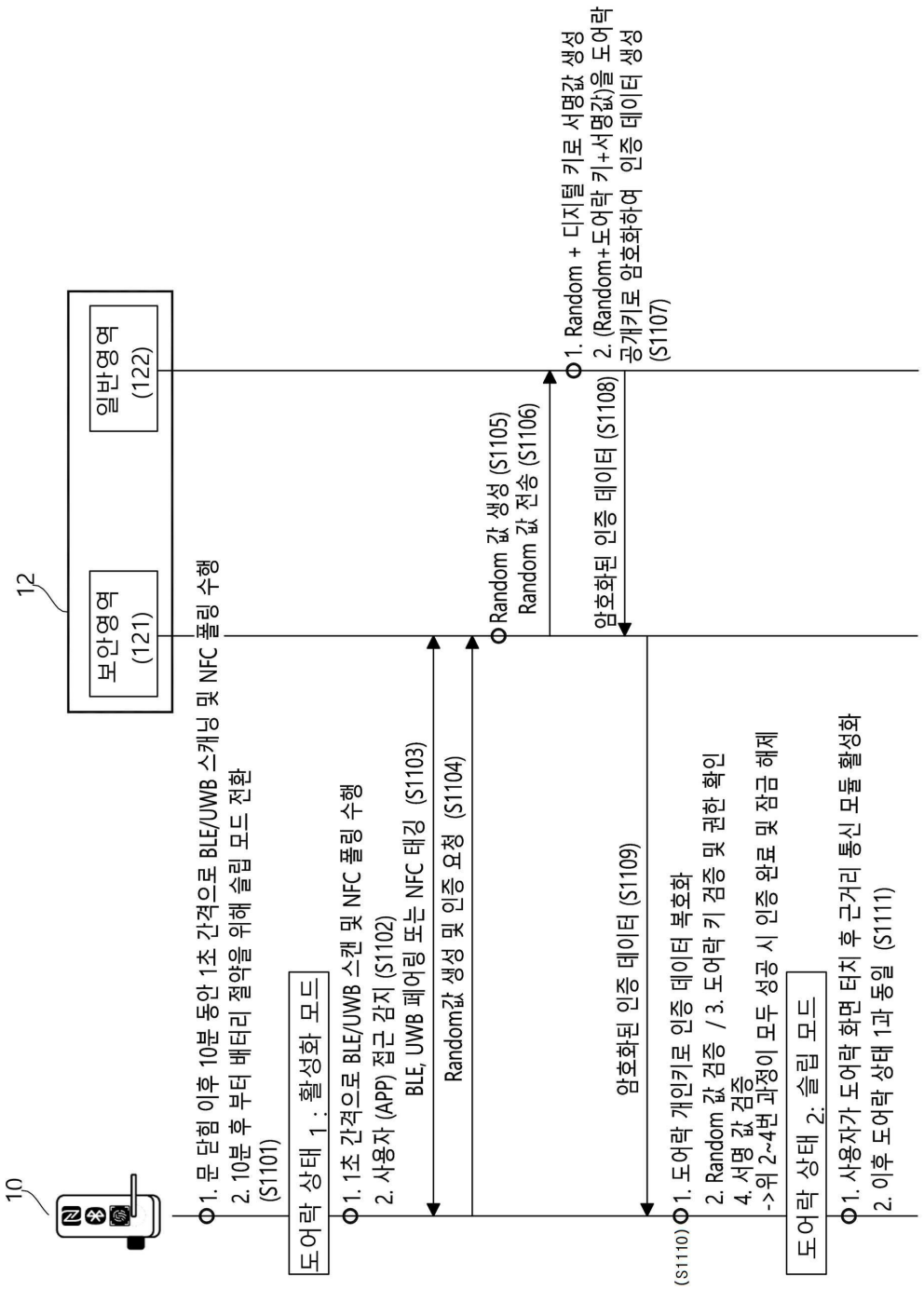
도면9


10
12
보안영역 (121)
일반영역 (122)
14
제어부 (141)
HSM (142)
DB (143)
도어락 뒷면 탈착 후 디지털 키 등록 버튼 선택 (S903)
통신 대기 상태 모드 유지 (S904)
QR촬영 또는 S/N 직접입력 (S905)
S/N 및 키 생성 요청 (S906)
1. Key pair 생성
2. 서버 공개키로 APP공개키 및 도어락 S/N 암호화 (S907)
암호화된 APP 공개키/도어락 S/N (S908)
암호화된 APP 공개키 /도어락 S/N (S909)
복호화 요청 (S910)
1. 서버 개인키로 복호화
2. S/N, APP 공개키 확인 (S911)
S/N 및 APP 공개키 (S912)
설정된 시간 단위로 NFC 풀링 및 BLE 스캔 (S913)
1. APP설치, 회원가입 및 로그인 완료 / 2. APP 최초 실행 후 도어락 등록 선택 (S901)
회원 정보 저장 (S902)

도면10


10
12
보안영역 (121)
일반영역 (122)
14
제어부 (141)
HSM (142)
DB (143)
S/N 확인, 도어락 공개키 확인 (S920)
S/N 존재? (S921)
N
Y : 디지털 키 생성 요청 (S923)
1. 디지털 키 생성
2. 생성된 디지털 키를 도어락 공개키로 암호화
3. 생성된 디지털 키 및 도어락 공개키를 APP 공개키로 암호화 (S924)
도어락 용 암호화 된 도어락용 키 및 APP용 암호화된 도어락키+도어락 공개키 (S925)
(S926)
미등록 도어락 안내 팝업후 APP종료 (S922)
APP 공개키로 암호화된 디지털 키 및 도어락 공개키 (S927)
APP 개인키로 복호화 및 저장 (S928)
근거리 통신(NFC, BLE 등)을 통한 도어락 공개키로 암호화된 도어키 전달 (S929)
Time out? (S930)
Y
N : 개인키로 암호화된 디지털 키 복호화 후 저장 (S932)
도어락 뒷면 등록 버튼 재 선택 후 근거리 통신 재시도 (S931)

도면11



도면12

랜덤 값	디지털 키	서명

【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 2

【변경전】

제 1 항에 있어서, 상기 사용자 인증정보를 입력 받는 단계는

사용자가 사용자 단말을 이용하여 도어락 디바이스에 포함된 QR 코드를 촬영하거나 도어락 디바이스에 기입된 도어락 S/N을 직접 입력하는 방식을 통해 사용자 인증정보를 입력 받는 것을 특징으로 하는 디지털키 등록방법.

【변경후】

제 1 항에 있어서, 상기 사용자 인증정보를 입력 받는 단계는

사용자가 사용자 단말을 이용하여 도어락 디바이스에 포함된 QR 코드를 촬영하거나 도어락 디바이스에 기입된 도어락 S/N을 직접 입력하는 방식을 통해 사용자 인증정보를 입력 받는 것을 특징으로 하는 도어락 키 등록방법.